



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.                                                            | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|----------------------------------------------------------------------------|-------------|----------------------|---------------------|------------------|
| 09/698,968                                                                 | 10/26/2000  | David Cheriton       | CISCP551            | 6471             |
| 26541                                                                      | 7590        | 09/02/2004           | EXAMINER            |                  |
| RITTER, LANG & KAPLAN<br>12930 SARATOGA AE. SUITE D1<br>SARATOGA, CA 95070 |             |                      | MAURO JR, THOMAS J  |                  |
|                                                                            |             |                      | ART UNIT            | PAPER NUMBER     |
|                                                                            |             |                      | 2143                |                  |

DATE MAILED: 09/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/698,968

Applicant(s)

CHERITON, DAVID

Examiner

Thomas J. Mauro Jr.

Art Unit

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 13 May 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-26 and 29-36 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-26 and 29-36 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892) ✓
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

1. Claims 1-26 remain pending. Claims 27 and 28 have been cancelled. Claims 29-36 have been newly added. A formal action on the merits of claims 1-26 and 29-36 follows.
2. Objection to the drawings along with the 112 2<sup>nd</sup> paragraph rejection have been withdrawn in light of the amendments made.

### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim 25 is rejected under 35 U.S.C. 102(e) as being anticipated by Vaid et al. (U.S. 6,502,131).

With respect to claim 25, Vaid teaches a method for propagating filters to an upstream device, comprising:

sending filter information to the upstream device [Vaid -- Col. 25 lines 47-49, lines 53-57 and lines 66-67 – Meta-policy service, running on server with monitoring tool software, distributes policies, i.e. filters, to intelligent agents, i.e. routers, switches, firewalls, etc, on

Art Unit: 2143

**the network, which inherently reside upstream from actual servers (See Figures 4, 5 and 16)];**

receiving flow information based on network flow received at the upstream device and analyzing said flow information [**Vaid -- Col. 10 lines 6-7, lines 11-12 and lines 41-47 -- Traffic monitored at upstream device is viewed and analyzed at downstream device, i.e. server. Therefore, the administrator receives, i.e. views, the flow information at the console]; and**

sending updated filter information to the upstream device [**Vaid -- Figure 8, Col. 10 lines 56-60, Col. 17 lines 37-43 and Col. 25 lines 66-67 -- After invoking policy, system continues to measure parameters and criteria to determine if policy should still be applied or not. Meta-policy service distributes and updates policies to intelligent agents, i.e. routers, switches, firewalls, etc, as policies are modified or changed, based upon statistics].**

### ***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-18 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaid et al. (U.S. 6,502,131) in view of Segal (U.S. 6,345,299).

Regarding claim 1, Vaid teaches a method for propagating filters to an upstream device comprising:

generating a filter at a first network device [Vaid -- Col. 10 lines 5-7, 11-12 and lines 56-60, Col. 14 lines 6-13 and lines 57-59 and Col. 17 lines 4-8 and lines 33-36 and Col. 23 lines 32-44 – Bandwidth management tool, running on a server, i.e. first network device namely the TrafficWare server, creates/specifies traffic policies, i.e. filters, to control the behavior of the traffic];

sending information on said filter to a second network device located upstream from said first network device [Vaid -- Col. 9 lines 34-36, Col. 10 lines 41-49, Col. 12 lines 23-32, Col. 25 lines 47-49, lines 53-57 and lines 66-67 – Meta-policy service, running on server with monitoring tool software, distributes policies, i.e. filters, to intelligent agents (second network devices), i.e. routers, switches, firewalls, etc, on the network, which would obviously reside upstream from the actual servers (See Figures 4, 5 and 16)];

requesting said second network device to install said filter [Vaid -- Col. 14 lines 6-13, Col. 17 lines 4-43, Col. 25 lines 66-67 and Col. 26 lines 50-54 – By using intelligent agents to actively participate in policy management, traffic policies, which are distributed to various network devices and enforced, requiring that the filter is installed at the node or point to enforce the policy]; and

analyzing new data received at said first network device and sending filter information to said second network device based on the analyzed data so that said second network device can refine the filter installed [Vaid -- Col. 6 lines 44-50, Col. 10 lines 27-40, Col. 15 lines 44-47

**and lines 65-67 and Col. 17 lines 23-57 – Monitors continually monitor network flow and adapt to “real” changes by deploying any policy modifications or activations to the various agents (second devices) which serve to implement the various network security policies distributed throughout the network, i.e. refining a filter].**

Vaid fails to explicitly teach filtering data closer to a source of said data and sending routing information from said first network device to said second network device so that the filter installed on said second network device filters traffic forwarded to said first network device without filtering traffic to other downstream nodes.

Segal, however, discloses a distributed security system of firewalls which propagates an e-mail filter from the receiving client to the various sending client firewalls to block the emails closer to their source [Segal -- **Figure 2, Col. 2 lines 64-67 – Col. 3 lines 1-15 and Col. 4 lines 1-26**]. In addition, Segal further teaches that the firewalls have route information, namely information concerning what other nodes are permitted to receive from and transmit to, which thereby limits transmissions to only their intended destinations and filters only the necessary packets going to a given node allowing other traffic to be unfiltered/blocked [Segal -- **Col. 2 lines 64-67 – Col. 3 lines 1-15 and lines 18-34 and Col. 4 lines 1-26**].

Vaid provides the creation/modifying/deploying of traffic policies and filters to various nodes on a network, in addition to teaching that the policies are distributed to multiple nodes on a network which ultimately helps provide a more autonomous and “self healing” system [Vaid -- **Col. 25 lines 11-21**].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the filtering of data closer to the source of the data along with

Art Unit: 2143

routing information so that only traffic forwarded to a first network device is filtered without filtering traffic to other downstream nodes, as taught by Segal into the invention of Vaid, in order to provide a more autonomous and “self healing” network which makes management less labor intensive and improves the timeliness and quality of the network and its management functions [Vaid -- Col. 25 lines 11-21].

Regarding claim 2, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 1 above, including wherein generating a filter at a first network device comprises automatically generating said filter based on network flow entering the device [Vaid - Col. 13 lines 57-67 and Col. 17 lines 23-26 and lines 33-37 – Upon detecting a given event or certain criteria being met, policy, i.e. filter, is automatically generated and put into effect].

Regarding claim 3, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 1 above, including receiving information based on monitored network flow and removing said filter from the first network device when the network flow requiring said filter is no longer present [Vaid -- Figure 8, Col. 10 lines 56-63 and Col. 17 lines 37-43 – After invoking policy, system continues to measure parameters and criteria to determine if policy should still be applied or not. If criteria does not warrant policy to continue, it would be removed through the continuous monitor, apply/modify filter and alert cycle].

Art Unit: 2143

Regarding claim 4, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 3 above, including requesting said upstream device to remove said filter **[Vaid -- Col. 25 lines 66-67 -- Meta-policy service distributes and updates policies to intelligent agents, i.e. routers, switches, firewalls, etc, as policies are created or changed. It is obvious that if a policy can be added or activated, it can be deactivated or removed].**

Regarding claim 5, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 1 above, including refining said filter at said first network device based on said monitored network flow **[Vaid -- Col. 10 lines 27-40 and lines 56-60 and Col. 17 lines 23-43 -- System continually cycles through measuring traffic, i.e. network, flow and applying applicable policies, thereby refining the policies implemented so that the proper one for the proper time with the proper measurements is put in place as "real" changes occur].**

Regarding claim 6, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 5 above, including requesting the upstream network device to refine said filter **[Vaid -- Col. 6 lines 44-50, Col. 10 lines 27-40, Col. 15 lines 44-47 and lines 65-67, Col. 17 lines 23-57 and Col. 25 lines 66-67 -- Monitors continually monitor network flow and adapt to "real" changes by deploying any policy modifications or activations to the various agents (second devices) which serve to implement the various network security policies distributed throughout the network, i.e. refining a filter. In addition, meta-policy**



**service distributes and updates policies to intelligent agents, i.e. routers, switches, firewalls, etc, as policies are created, changed or refined].**

Regarding claim 7, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 1 above, including wherein generating a filter comprises detecting potentially harmful network flows and generating a filter to prevent packets corresponding to said detected potentially harmful network flows from passing through said second network device [**Vaid -- Col. 11 lines 1-12 and Col. 28 lines 37-40 – Harmful network flows, such as traffic bursts, can cause a server to crash or not allow critical traffic to get through the network. Intelligent agents, i.e. routers, switches, firewalls, etc, have the ability, depending on the policy sent to them, to block/drop/queue or modify packets].**

Regarding claim 8, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 7 above, including wherein generating filters further comprises classifying network flow based on a source device sending a packet [**Vaid -- Col. 27 lines 34-39 – Policies, i.e. filters, define monitoring and control actions, which can be classified by source, i.e. device sending packet].**

Regarding claim 9, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 8 above, including wherein the network flow is classified based on an address of the source device [**Vaid -- Col. 10 lines 17-22 – Monitoring of network traffic flow**

---

Art Unit: 2143

**is classified in numerous ways, one of which is by source address of device sending packets].**

Regarding claim 10, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 1 above, including wherein generating filters comprises analyzing network flow entering said first network device [**Vaid -- Col. 10 lines 41-47 – Network flow can be monitored at one or more nodes on the network, including the main monitoring server, i.e. first network device, and intelligent agents such as routers, switches, firewalls, etc...].**

Regarding claim 11, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 10 above, including wherein analyzing said network flow is performed by software [**Vaid -- Figure 9 (traffic monitoring application) and Col. 10 lines 2-5 – Monitoring tool is software based].**

Regarding claim 12, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 10 above, including selecting a class of network flows to analyze based on previously analyzed network flows [**Vaid -- Col. 10 lines 56-60 and Col. 17 lines 33-43 – After a policy is invoked, measurements regarding the invocation of that particular policy continue to be taken, i.e. class of networks flows are analyzed based upon past analyzed network flows, to ensure policy needs to remain in place as network conditions change].**

---

Regarding claim 13, Vaid teaches a computer program product for propagating a filter to an upstream device [**Vaid -- Col. 3 lines 25-29, lines 55-57 and Col. 3 lines 66-67 – Col. 4 line 1 – Software runs management tool which is responsible for creating and invoking policies which are then distributed to intelligent agents**]. The remaining limitations in claim 13 are similar to the limitations in claim 1. Therefore, they are rejected under the same rationale.

Regarding claim 14, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 13 above, including wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and data signal embodied in a carrier wave [**Vaid -- Col. 3 lines 25-29 – Software management tool, which is responsible for creating and invoking policies, is stored in computer memory**].

Regarding claim 15, this is a computer program product claim corresponding to the method claimed in claim 7. It has similar limitations; therefore, claim 15 is rejected under the same rationale.

Regarding claims 16-17, these are computer program product claims corresponding to the methods claimed in claims 3-4. They have similar limitations; therefore, claims 16-17 are rejected under the same rationale.

Art Unit: 2143

Regarding claim 18, this is a system claim corresponding to the method claimed in claim

1. It has similar limitations; therefore, claim 18 is rejected under the same rationale.

Regarding claim 36, Vaid-Segal teach the invention substantially as claimed, as  
aforementioned in claim 1 above, including wherein a filter propagation protocol is utilized to  
exchange information between devices and modify said filters [**Vaid -- Col. 23 lines 40-42 --  
Policies are communicated to other devices, i.e. propagated, using a policy exchange  
protocol, i.e. filter propagation protocol.**]

7. Claims 19, 21-24 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over  
Vaid et al. (U.S. 6,502,131) in view of Jackowski et al. (U.S. 6,141,686).

Regarding claim 19, Vaid teaches a method of installing filters on connected network  
devices, comprising:

analyzing network flows received at a first network device [**Vaid -- Col. 10 lines 41-47 --  
Management tool allows monitoring of one or more nodes, i.e. devices, such as servers,  
routers, switches, firewalls, etc, i.e. first network device**];

generating a filter at a second network device based on said analyzed flows [**Vaid -- Col.  
6 lines 44-50, Col. 10 lines 27-40, Col. 15 lines 44-47 and lines 65-67 and Col. 17 lines 23-57  
-- Monitors continually monitor network flow and adapt to "real" changes by deploying**

**any policy modifications or activations to the various agents (second devices) which serve to implement the various network security policies distributed throughout the network, i.e. refining a filter];**

propagating said filter from the second network device to the first network device [**Vaid - Col. 9 lines 34-36, Col. 10 lines 41-49, Col. 12 lines 23-32, Col. 25 lines 47-49, lines 53-57 and lines 66-67 – Meta-policy service, running on server with monitoring tool software, distributes policies, i.e. filters, to intelligent agents (second network devices), i.e. routers, switches, firewalls, etc, on the network, which would obviously reside upstream from the actual servers (See Figures 4, 5 and 16)]; and**

utilizing a filter propagation protocol to exchange information directly between the first and second network devices to refine said filter [**Vaid -- Col. 23 lines 40-42 – Policies are communicated to other devices, i.e. propagated, using a policy exchange protocol, i.e. filter propagation protocol].**

Vaid, while communicating information between devices, fails to explicitly teach generating filter statistics at a second network device and sending the statistics to the first network device.

Jackowski, however, discloses generating filter statistics, namely bandwidth information at a first edge device and communicating that information to a policy server [**Jackowski -- Col. 2 lines 60-67 – Col. 3 lines 1-10].**

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the generation and sending of filter statistics, as taught by Jackowski into the invention of Vaid, in order to further improve the quality of network management and more effective implementations of filter policies [**Vaid -- Col. 25 lines 11-21].**

Regarding claim 21, Vaid teaches a method for updating filters on a device, comprising:  
receiving data at an upstream device [**Vaid -- Figure 4 and Col. 2 lines 59-61 – Flow of information is received at an upstream device, i.e. router, switch, firewall, etc...]**;

filtering at least a portion of the data before sending the data to a downstream device [**Vaid -- Col. 25 lines 47-49, lines 53-57, lines 66-67 and Col. 28 lines 37-40 – Meta-policy service, running on server with monitoring tool software, distributes policies, i.e. filters, to intelligent agents, i.e. routers, switches, firewalls, etc, on the network, which then actively participate in enforcing, i.e. filtering, data before heading downstream]**;

receiving filter information from the downstream device [**Vaid -- Col. 25 lines 47-49, lines 53-57 and lines 66-67 – Meta-policy service, running on server with monitoring tool software, distributes policies, i.e. filters, to intelligent agents, i.e. routers, switches, firewalls, etc, on the network, which inherently reside upstream from actual servers (See Figures 4, 5 and 16)]**; and updating a filter installed on the upstream device [**Vaid -- Col. 6 lines 44-50, Col. 10 lines 27-40, Col. 15 lines 44-47 and lines 65-67 and Col. 17 lines 23-57 – Monitors continually monitor network flow and adapt to “real” changes by deploying any policy modifications or activations to the various agents (second devices) which serve to implement the various network security policies distributed throughout the network, i.e. refining a filter]**.

Vaid, while communicating information between devices, fails to explicitly teach generating filter statistics at a second network device and sending the statistics to the first network device.

Jackowski, however, discloses generating filter statistics, namely bandwidth information at a first edge device and communicating that information to a policy server [**Jackowski -- Col. 2 lines 60-67 -- Col. 3 lines 1-10**].

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the generation and sending of filter statistics, as taught by Jackowski into the invention of Vaid, in order to further improve the quality of network management and more effective implementations of filter policies [**Vaid -- Col. 25 lines 11-21**].

Regarding claim 22, Vaid-Jackowski teach the invention substantially as claimed, as aforementioned in claim 21 above, including wherein receiving filter information comprises using a filter propagation protocol [**Vaid -- Col. 23 lines 40-42 -- Policies are communicated to other devices, i.e. propagated, using a policy exchange protocol, i.e. filter propagation protocol**].

Regarding claim 23, Vaid-Jackowski teach the invention substantially as claimed, as aforementioned in claim 22 above, including wherein the filter propagation protocol is operable to create, remove, or modify existing filters [**Vaid -- Figure 8, Col. 10 lines 56-60 and Col. 17 lines 37-43 -- System has ability to create, i.e. invoke policy upon which system continues to measure parameters and criteria to determine if policy should still be applied or not. If criteria does not warrant policy to continue, it would be removed. Also, policy can be changed, i.e. modified, if monitoring conditions are changed by applying another filter**].

Regarding claim 24, Vaid-Jackowski teach the invention substantially as claimed, as aforementioned in claim 22 above, including wherein the filter propagation protocol uses negative routing [**Vaid -- Col. 10 lines 56-60, Col. 17 lines 23-43 and Col. 28 lines 37-40 – System allows all packets to be routed to their proper location unless measurements cause a policy to be invoked causing certain packets not to be forwarded, i.e. negative routing**].

Regarding claim 29, Vaid-Jackowski teach the invention substantially as claimed, as aforementioned in claim 19 above, including monitoring the system over predefined intervals, i.e. time frequencies, such as day to day, weekly, etc. [**Vaid -- Col. 11 lines 42-48**].

It would have been obvious that if filters can be installed on a device that filters can be reinstalled on a device, as this is just duplicating the installation process.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include the reinstalling of a filter at predetermined intervals, as taught by Vaid, in order to ensure the filters are functioning properly and that the proper network traffic is being filtered.

8. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaid et al. (U.S. 6,502,131) and Jackowski et al. (U.S. 6,141,686), as applied to claim 19 above, in view of Segal (U.S. 6,345,299).

---



Art Unit: 2143

Regarding claim 20, Vaid-Jackowski teach the invention substantially as claimed, as aforementioned in claim 19 above, including propagating filters [**Vaid -- Col. 9 lines 34-36, Col. 10 lines 41-49, Col. 12 lines 23-32, Col. 25 lines 47-49, lines 53-57 and lines 66-67 -- Meta-policy service, running on server with monitoring tool software, distributes policies, i.e. filters, to intelligent agents (second network devices), i.e. routers, switches, firewalls, etc, on the network, which would obviously reside upstream from the actual servers (See Figures 4, 5 and 16)**].

Vaid-Jackowski fail to teach propagating filter information such that said filter is positioned closer to a source of said flows.

Segal, however, discloses a distributed security system of firewalls which propagates an e-mail filter from the receiving client to the various sending client firewalls to block the emails closer to their source [**Segal -- Figure 2, Col. 2 lines 64-67 -- Col. 3 lines 1-15 and Col. 4 lines 1-26**]. In addition, Segal further teaches that the firewalls have route information, namely information concerning what other nodes are permitted to receive from and transmit to, which thereby limits transmissions to only their intended destinations and filters only the necessary packets going to a given node allowing other traffic to be unfiltered/blocked [**Segal -- Col. 2 lines 64-67 -- Col. 3 lines 1-15 and lines 18-34 and Col. 4 lines 1-26**].

Vaid provides the creation/modifying/deploying of traffic policies and filters to various nodes on a network, in addition to teaching that the policies are distributed to multiple nodes on a network which ultimately helps provide a more autonomous and "self healing" system [**Vaid -- Col. 25 lines 11-21**].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the

invention was made to incorporate the filtering of data closer to the source of the data along with routing information so that only traffic forwarded to a first network device is filtered without filtering traffic to other downstream nodes, as taught by Segal into the invention of Vaid, in order to provide a more autonomous and “self healing” network which makes management less labor intensive and improves the timeliness and quality of the network and its management functions **[Vaid -- Col. 25 lines 11-21]**.

9. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaid et al. (U.S. 6,502,131), as applied to claim 25 above, in view of Chiu et al. (U.S. 5,883,901).

Regarding claim 26, Vaid teaches the invention substantially as claimed, as aforementioned in claim 25 above, but fails to teach keeping count of received packets and dropped packets.

Chiu, however, teaches a router which keeps track of received packets and the number of dropped packets **[Chiu -- Col. 30 lines 43-54]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate counting of received and dropped packets, as taught by Chiu into the invention of Vaid, in order to provide greater statistical data and flexibility to make better informed decisions upon which policies to activate at a given time.

---

10. Claims 30-31 and 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaid et al. (U.S. 6,502,131) in view of Dietz et al. (U.S. 6,665,725).

Regarding claim 30, Vaid teaches a method for propagating filters between a first network device and a second network device located upstream of the first network device, the method comprising:

receiving filter information from the first network device at the second network device  
**[Vaid -- Col. 25 lines 47-49, lines 53-57 and lines 66-67 -- Meta-policy service, running on server with monitoring tool software, distributes policies, i.e. filters, to intelligent agents, i.e. routers, switches, firewalls, etc, on the network, which inherently reside upstream from actual servers (See Figures 4, 5 and 16)];**

generating and installing a filter at the second network device based on the filter information **[Vaid -- Col. 10 lines 5-7, 11-12 and lines 56-60, Col. 14 lines 6-13 and lines 57-59, Col. 17 lines 4-43, Col. 23 lines 32-44, Col. 25 lines 66-67 and Col. 26 lines 50-54 -- Bandwidth management tool, running on a server, i.e. first network device namely the TrafficWare server, creates/specifies traffic policies, i.e. filters, to control the behavior of the traffic. By using intelligent agents to actively participate in policy management, traffic policies, which are distributed to various network devices and enforced, requiring that the filter is installed at the node or point to enforce the policy];**

classifying network flow received at the second network device **[Vaid -- Col. 8 lines 10-58 and Col. 14 lines 33-56 -- Packets are classified by a wide variety of classifications in order to determine the amount of bandwidth or QoS requirements];**

modifying said filter installed at the second network device [**Vaid -- Col. 6 lines 44-50, Col. 10 lines 27-40, Col. 15 lines 44-47 and lines 65-67 and Col. 17 lines 23-57 – Monitors continually monitor network flow and adapt to “real” changes by deploying any policy modifications or activations to the various agents (second devices) which serve to implement the various network security policies distributed throughout the network, i.e. modifying a filter**]; and

transmitting data from the second network device to the first network device so that the first network device can modify the filter installed [**Vaid -- Col. 23 lines 40-42 – Policies are communicated to other devices, i.e. propagated, using a policy exchange protocol, i.e. filter propagation protocol**].

Vaid fails to explicitly teach performing a lookup in a flow cache, building a new entry in the cache if the network flow is not found, generating a flow record based on the network flow and analyzing the flow record with previously generated flow records.

Dietz, however, teaches a packet monitoring system which parses and analyzes the flow of packets by performing a lookup in a flow cache, building a new entry in the cache if the flow is not found, generating a flow record based on the network flow and analyzing the flow record with previously generated flow records [**Dietz -- Col. 10 lines 35-67 – Col. 12 lines 1-12 and Col. 23 lines 47-50**].

Both Dietz and Vaid are concerned with classifying and monitoring packet flows across a network.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the performing a lookup in a flow cache, building a new entry

Art Unit: 2143

in the cache if the network flow is not found, generating a flow record based on the network flow and analyzing the flow record with previously generated flow records, as taught by Dietz into the invention of Vaid, in order to provide a mechanism to describe state operations to perform on packets **[Dietz -- Col. 3 lines 55-58]** in addition to providing a storage that allows efficient searching of packet flow records **[Dietz -- Col. 10 lines 37-39]**.

Regarding claim 31, Vaid-Dietz teach the invention substantially as claimed, as aforementioned in claim 30 above, including classifying network flow based on an access control list **[Vaid -- Col. 14 lines 34-55 and Col. 24 lines 58-64 – Access control lists give the available services and the hosts which can use the services. Here Vaid teaches that traffic classes consist of a combination of IP address, for example a user's IP address and services, i.e. FTP HTTP, etc. Thus it is obvious that access can be controlled based upon a correlation of the service, i.e. FTP, and the users, i.e. IP addresses, which can use it]**.

Regarding claim 33, Vaid-Dietz teach the invention substantially as claimed, as aforementioned in claim 30 above, including wherein analyzing network flow comprises analyzing aggregate summary records **[Dietz -- Col. 17 lines 43-61 – Statistics, which are an aggregation of all flow records, are analyzed to determine network usage and quality of service]**.

Regarding claim 34, Vaid-Dietz teach the invention substantially as claimed, as aforementioned in claim 30 above, including wherein analyzing said flow comprises monitoring

Art Unit: 2143

statistics associated with the installed filter [**Dietz -- Col. 17 lines 43-61 – Statistics are record and analyzed to monitor the flow of packets within a network**].

11. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaid et al. (U.S. 6,502,131) and Dietz et al. (U.S. 6,665,725), as applied to claim 30 above, in view of Coss et al. (U.S. 6,098,172).

Regarding claim 32, Vaid-Dietz teach the invention substantially as claimed, as aforementioned in claim 30 above, but fails to explicitly teach classifying only a limited number of packets received in the flow.

Coss, however, teaches a computer network firewall which implements stateful packet filtering by passing subsequent packets from a same network session without applying a rule set, i.e. classifying, the packets again [**Coss -- Col. 5 lines 41-56**].

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the classifying only a limited number of packets, as taught by Coss into the invention of Vaid-Dietz, in order to provide performance performances over conventional packet classifying/filtering [**Coss -- Col. 5 lines 54-56**].

12. Claim 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaid et al. (U.S. 6,502,131) and Segal (U.S. 6,345,299), as applied to claim 1 above, in view of Tang et al. (US 2003/0165140).

Regarding claim 35, Vaid-Segal teach the invention substantially as claimed, as aforementioned in claim 1 above, but fail to explicitly teach utilizing a reverse path forwarding at a network device.

Tang, however, discloses a multicast distribution system which employs Reverse Path Forwarding (RPF) to check on the source of received messages [Tang -- Page 2 paragraph [0013] and page 9 paragraph [0081]].

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the use of Reverse Path Forwarding (RPF), as taught by Tang into the invention of Vaid-Segal, in order to check the validity/duplication of a message received by checking the source channel it was received on [Tang -- Page 2 paragraph [0013]].

#### ***Response to Arguments***

13. Applicant's arguments with respect to claims 1, 13, 18, 19 and 21 have been considered but are moot in view of the new ground(s) of rejection.

14. Applicant's arguments filed 5/13/2004 have been fully considered but they are not persuasive.

(A) Applicant contends that Vaid does not disclose the exchanging of filter information between nodes in order to be updated, whereas claim 25 calls for this limitation.

In response to argument A, Examiner asserts that Vaid discloses updating filters based upon flow data received at a monitored device [**Vaid -- Col. 6 lines 44-50, Col. 10 lines 27-40, Col. 15 lines 44-47 and lines 65-67 and Col. 17 lines 23-57 – Monitors continually monitor network flow and adapt to “real” changes by deploying any policy modifications or activations to the various agents (second devices) which serve to implement the various network security policies distributed throughout the network, i.e. refining a filter**]. In addition, Administrators, or other privileged users can view profiling and monitored traffic information via a GUI console in deciding if a new security policy should be implemented or to chart current policies [**Vaid -- Col. 17 lines 58-67 – Col. 18 lines 1-14 and Col. 27 lines 23-40**]. Thus, filter information is exchanged between a monitoring node, i.e. router or switch, and a server or administrator node. Thus, the Examiner accordingly demurs to this assertion as filter information is exchanged between nodes.



***Conclusion***

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Nessel et al. (U.S. 5,968,176) discloses a multilayer firewall system with security agents deployed on multiple network devices.

16. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas J. Mauro Jr. whose telephone number is 703-605-1234. The examiner can normally be reached on M-F 8:00a.m. - 4:30p.m..

Art Unit: 2143

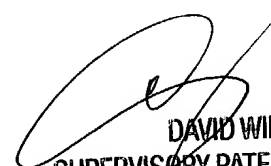
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on 703-308-5221. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



TJM

August 27, 2004



DAVID WILEY  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100